# Organization of Information Security Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to ensure a framework is in place to include information security within internal and remote operations.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Organization of Information Security Policy applies to all business processes and data, information systems and components, personnel, and physical areas of [Insert Company’s Name].

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws, Regulations, and Standards

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
| ISO27001:2013 | A.6 (A.6.1, A.6.2) |
| NIST SP 800-53 v4 | XX-1 controls, PM-1~PM-3, CP-2, CP-4, IR-4, PL-1, PS-7, SA-3, SA-9, CA-1~CA-3, CA-6, PL-4, PS-6, SA-9, IR-4, IR-6, IR-7, PE-13, SA-19, SI-5, PM-15, SI-5, PM-9, CA-7, SA-11, AC-20, RA-3, SA-9, AC-8, AT-2, AT-3, PL-4, SA-9, PL-4, PS-6, PS-7 |

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

**Management Commitment to Information Security:**

* + Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
  + Top management should ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.
  + Top management should also assign responsibilities and authorities for reporting performance of the information security management system within the organization.

**Internal Organization:**

* + All responsibilities and behaviors relating to information security must be clearly defined.
    - A clear and appropriate security organizational structure should be documented and communicated within the organization and to other interested parties.
    - An information security officer will be determined and the role will be assigned appropriately.
    - Segregation of duties will be implemented to ensure minimal crossover.
  + Contacts with the appropriate authorities will be identified and maintained.
  + Appropriate contacts with special interest groups or specialist security forums will be maintained.
  + Project management will include information security as a crucial consideration regardless of the type of project.
  + [Insert Company’s Name] should:
    - Determine the necessary competence of person(s) doing work under its control that affects its information security performance.
    - Ensure that these persons are competent on the basis of appropriate education, training, or experience.
    - Where applicable, take actions to acquire the necessary competence and evaluate the effectiveness of the actions taken.
    - Retain appropriate documented information as evidence of competence.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.